

February 8, 2016

Richard Cavanagh, PhD
Acting Associate Director for Laboratory Programs
National Institute of Standards and Technology
Department of Commerce
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Dr. Cavanagh:

On behalf of the Healthcare Information and Management Systems Society ([HIMSS](http://www.himss.org)), we are pleased to provide written comments regarding [Views on the Framework for Improving Critical Infrastructure Cybersecurity](#), Docket Number: 151103999-5999-01, which was published in the Federal Register on December 11, 2015. HIMSS appreciates the opportunity to comment on this Request for Information (RFI), and we look forward to continuing our dialogue with the National Institute of Standards and Technology (NIST) on how health information technology (IT) can play a role in improving our nation's cybersecurity infrastructure.

Included below are our answers to the relevant questions to HIMSS from the RFI:

Describe your organization and its interest in the Framework.

HIMSS is a global, cause-based, not-for-profit organization focused on better health through information technology (IT). In North America, HIMSS focuses on health IT thought leadership, education, market research, and media services. Founded in 1961, HIMSS North America encompasses more than 64,000 individuals, of which more than two-thirds work in healthcare provider, governmental, and not-for-profit organizations, plus over 640 corporations and 450 not-for-profit partner organizations, that share this cause.

Healthcare, a critical infrastructure sector in the United States, requires meaningful, secure e-exchange of health information to improve health, provide better care, and lower costs. Healthcare providers and organizations must be equipped to defend against growing cyber threats using a consistent and effectively-implemented data security framework. HIMSS applauds NIST's efforts in developing the NIST Cybersecurity Framework in collaboration with the private sector.

HIMSS has provided input to the NIST Cybersecurity Framework since its inception. HIMSS has participated in the NIST Cybersecurity Framework workshops. Further, HIMSS has submitted comments in response to the two previous RFIs (i.e., [comments to the NIST Cybersecurity Preliminary Framework](#) and [comments to the NIST on Cybersecurity Infrastructure Framework RFI](#)). Now that the Cybersecurity Act of 2015 (CSA) has been signed into law, and the importance of Section 405 of the new law to the healthcare sector, HIMSS

offers our comments in light of this law’s reference to “a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes.” The NIST Cybersecurity Framework could potentially be leveraged in this direction.

Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.

While HIMSS does not directly use the Framework, HIMSS is providing this response both in view of its subject matter expertise and input from its members. HIMSS privacy and security volunteers have generally had awareness of the Framework, but not widespread adoption or use of the same.

What portions of the Framework are most useful?

Generally, the Framework serves to inform organizations that are in need of either creating or updating their own risk management program. Whether an organization is standing up a new cybersecurity program or has a sophisticated program already in place, the Framework has the potential to serve organizations well in advancing the capabilities of organizations in addressing cybersecurity risk.

The Framework Core provides a set of functions (i.e., activities and outcomes) that organizations, including healthcare organizations, need to implement to address security incidents and, generally, managing cybersecurity risk: (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover.

Moreover, the Framework focuses on developing a risk management process and guides organizations through a five step process: (1) Describe the current cybersecurity posture, (2) Describe the target state for cybersecurity, (3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process, (4) Assess progress toward the target state, and (5) Communicate among internal and external stakeholders about cybersecurity risk.

Since many healthcare organizations could benefit from improving their risk management process and better address cybersecurity risk, the Framework could be useful in helping healthcare organizations improve their security posture.

What portions of the Framework are least useful?

Section 2.3 (“Framework Profile”): The Framework does not adequately define what the “Target Profile” of an organization should be. While it is important for an organization have a desired target state, it is also equally important for an organization to know what target state, ideally, it should achieve. Some organizations may either lack the know-how to determine this on their own, or may benefit from specific guidance on what this target state should be—especially in the day and age of targeted, sophisticated, advanced, and persistent threats. It needs to be emphasized that even the best cybersecurity programs, with the most skilled cybersecurity personnel, may not always prevail against sophisticated threat actors, such as nation states and

organized cybercriminal groups. For this reason, the healthcare sector as a whole would greatly benefit from a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes as provided for in CSA. Even the most sophisticated cyber threats by nation state actors can be defended against, especially with the healthcare sector stakeholders and government working together as a cohesive whole to effectively and meaningfully share cyber threat-related information.

On a related note, while gap analysis is discussed and can be a great aid in helping an organization achieve greater resiliency, the Framework Profile lacks metrics and other tools set forth in the Framework to help organizations gauge current status and goal state. Accordingly, metrics and other tools need to be added to this section and other sections, as appropriate, so that adopters of the Framework can objectively measure progress.

Sections 3.0 through 3.5 (“Use of the Framework”): The Framework could be greatly enhanced to benefit the healthcare sector by making the subsection more sector-specific. This would aid in the adoption and implementation of the Framework by healthcare stakeholders.

For example, the Framework does not define what a Target Profile should be. The healthcare sector could benefit from specific guidance from NIST (with input from healthcare stakeholders) on what an ideal “Target Profile” would be for a healthcare organization. Further, healthcare stakeholders could collaborate with NIST to develop what this should be, based upon consensus across the healthcare sector. This would be consistent with the objectives of Section 405 of CSA.

Moreover, the Framework could be more useful to healthcare stakeholders by providing metrics and other tools to measure progress with the Framework. By having such metrics and tools, Framework users could gain an objective perspective on current status and progress toward higher readiness. Metrics and other tools, as appropriate, should be incorporated into Sections 3.0 through 3.5. These metrics and tools will not only help organizations improve their target state in terms of its cybersecurity efforts, but also improve resiliency against future cyber-attacks and other cybersecurity incidents (especially as a result of doing a gap analysis and incorporating the lessons learned).

By way of example, a maturity model implemented and deployed by stakeholders in the electrical sector is the [Electricity Subsector Cybersecurity Maturity Model](#) (ES-C2M2). Within each domain (which includes information sharing and communication event and incident response, continuity of operations, workforce management, and cybersecurity program management), there are objectives and associated practices for each maturity indicator level. Maturity indicator levels are cumulative—practices must be performed by the organization at the current maturity indicator level and the preceding maturity indicator levels associated with the particular domain. The organization will progress until it reaches a target maturity indicator level which it has set for the particular domain.

By a similar token, the healthcare sector could benefit from adopting and implementing a maturity model, which is private sector-led and consensus-based, and further includes guidelines, best practices, methodologies, procedures, and processes as provided for by Section 405 of CSA.

In this vein, healthcare stakeholders could benefit from tracking progress with the maturity model, adopting and implementing practices commensurate with the current level of maturity in each cybersecurity program domain of the cybersecurity maturity model.

Section 3.5: Methodology to Protect Privacy and Civil Liberties: HIMSS applauds NIST for addressing protecting privacy and civil liberties. However, HIMSS also notes that privacy risk management is equally as important as information security risk management to healthcare organizations, as well as others. Organizations, including healthcare organizations, may benefit from an in-depth discussion in the Framework about the intersection between privacy risk management and information security risk management.

Harmful effects, including data loss and damage to IT systems and/or the organization, can be mitigated with effective privacy and security risk management. This means effective collaboration, communication, and processes between the privacy and information security functions at the organization.

Moreover, the healthcare sector could benefit from a common set of consensus-based, private sector-led guidelines, best practices, methodologies, procedures, and processes in relation to privacy and information security risk management, consistent with Section 405 of CSA. Thus, the Framework could be greatly enhanced in this area.

Has your organization’s use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?

Based upon input from its members, HIMSS infers that there is modest awareness of the Framework in the healthcare sector. Moreover, the healthcare sector lacks a common set of voluntary, consensus-based, and healthcare private sector-led guidelines, best practices, methodologies, procedures, and processes, which would be consistent with Section 405 of CSA. The Framework could be used as a tool to achieve this goal.

What steps should be taken to “prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes” as required by the Cybersecurity Enhancement Act of 2014?

The NIST Cybersecurity Framework should continue to be voluntary, consistent with Section 405 of CSA.

Should the Framework be updated? Why or why not?

In view of [Executive Order 13636](#) and the goal of achieving security and resiliency of critical infrastructure sector organizations, the Framework should be updated, based upon input from stakeholders, including in the healthcare industry. Moreover, cybersecurity is a moving target. Our collaborative approach to cybersecurity needs to continually be updated as well to stay ahead of cyber threats that exist, now and into the future.

Prospectively, the Framework could be used as a tool to develop a common set of voluntary, consensus-based, and private sector-led guidelines, best practices, methodologies, procedures, and processes, consistent with Section 405 of CSA. However, the Framework would need to be updated to incorporate such information in order to achieve this goal. In view of the foregoing, the Framework could be greatly enhanced to benefit the healthcare sector.

In a similar vein, HIMSS suggests that NIST (with input from healthcare stakeholders) bring together government, academia, and industry to continue to evolve the Framework that remains fluid and flexible enough to be a living document that can be improved to ensure that the Framework content reflects real world risks and risk management, including in view of interdependencies among the critical infrastructure sectors.

What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.

Generally, the Framework could be used as a tool to develop a common set of voluntary, consensus-based, and private sector-led guidelines, best practices, methodologies, procedures, and processes, consistent with Section 405 of CSA. In addition, the Framework could be greatly enhanced to benefit the healthcare sector. This could be achieved by adding context specific to the healthcare sector in each of the substantive sections, including Section 3.0 through 3.5 (“How to Use the Framework”), or in an addendum.

Section 2.3 (“Framework Profile”): As stated earlier in our response, the Framework does not adequately define what the “Target Profile” of an organization should be. While it is important that an organization have a desired target state, it is also equally important for an organization to know what target state, ideally, it should achieve. Some organizations may either lack the savvy or know-how to determine this on their own, or may benefit from specific guidance on what this target state should be—especially in the day and age of targeted, sophisticated, advanced, and persistent threats. Based upon input from its members, HIMSS infers that there is modest awareness of the Framework in the healthcare sector. Moreover, as the healthcare sector lacks a common set of voluntary, consensus-based, and healthcare private sector-led guidelines, best practices, methodologies, procedures, and processes, consistent with Section 405 of CSA. The Framework could be used as a tool to achieve this goal.

On a related note, while gap analysis is discussed and can be a great aid in helping an organization achieve greater resiliency, there are no metrics or other tools set forth in the Framework to help organizations gauge where they are vis-à-vis where they need to be. Accordingly, metrics and other tools need to be added to this section and other sections, as appropriate, so that adopters of the Framework can objectively measure their progress.

Sections 3.0 through 3.5 (“Use of the Framework”): The Framework could be greatly enhanced to benefit the healthcare sector by making it more sector-specific. This would aid in the adoption and implementation of the Framework by healthcare stakeholders.

For example, the Framework does not define what a Target Profile should be. The healthcare sector could benefit from specific guidance from NIST (with input from healthcare stakeholders)

on what an ideal “Target Profile” would be for a healthcare organization. Further, healthcare stakeholders could collaborate with NIST to develop what this should be, based upon consensus across the healthcare sector.

Moreover, the Framework could be more useful to healthcare stakeholders by providing metrics and other tools to measure progress with the Framework. For example, the healthcare sector could benefit from adopting and implementing a maturity model, which is private sector-led and consensus-based, and further includes guidelines, best practices, methodologies, procedures, and processes as provided for by Section 405 of CSA. By having such metrics and tools, users of the Framework can gain an objective perspective on how far away they are from where they need to be. Metrics and other tools, as appropriate, should be incorporated into Sections 3.0 through 3.5. These metrics and tools will not only help organizations improve their target state in terms of its cybersecurity efforts, but also improve resiliency against future cyber-attacks and other cybersecurity incidents as well (especially as a result of doing a gap analysis and incorporating the lessons learned).

Section 3.5: Methodology to Protect Privacy and Civil Liberties: HIMSS applauds NIST for addressing protecting privacy and civil liberties. However, HIMSS also notes that privacy risk management is equally as important as information security risk management to healthcare organizations, as well as others. Organizations, including healthcare organizations, may benefit from an in-depth discussion in the Framework about the intersection between privacy risk management and information security risk management.

Harmful effects, including data loss and damage to IT systems and/or the organization, can be greatly lessened with effective privacy and security risk management. This means effective collaboration, communication, and processes between the privacy and information security functions at the organization.

As stated earlier, the healthcare sector could benefit from a common set of consensus-based, industry-led guidelines, best practices, methodologies, procedures, and processes in relation to privacy and information security risk management. Thus, the Framework could be greatly enhanced in this area.

Glossary: The glossary should be expanded to include other terms of art as used in the Framework (in its current and future iterations). For example, in its current state, the glossary could be enhanced by defining the term “cybersecurity incident.”

Are there additions, updates or changes to the Framework’s references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?

Any additions, updates, or changes to the Framework, in order to make it more healthcare-sector specific, should be made through a collaborative process that includes a wide array of healthcare sector stakeholders. .

Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?

Dependencies upon other sectors must be taken into account in updating the Framework in order for organizations to be resilient against cyber-attacks and other security incidents. Reference should be made to the relevant annex of the National Infrastructure Protection Plan (e.g., [Healthcare and Public Health Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan](#) (2010)) and the National Cyber Incident Response Plan. In other words, a multi-dimensional approach to defense from cyber-attacks and other security incidents must be carefully examined and addressed, especially for critical infrastructure sectors such as healthcare, which has a touchpoint to many other sectors. Also as mentioned above, any additions, updates, or changes to the Framework in order to make it more healthcare-sector specific should be made through a collaborative process that includes a wide array of healthcare sector stakeholders.

Should developments made in the nine areas identified by NIST in its Framework-related “Roadmap” be used to inform any updates to the Framework? If so, how?

Authentication

Developments made in the area of authentication, including multi-factor authentication, as outlined in the Roadmap should be included in updates to the Framework and specifically in Section 3 of the Framework (“Use of the Framework”).

Section 3.5 entitled “Methodology to Protect Privacy and Civil Liberties” does have a subsection entitled “Approaches to identifying and authorizing individuals to access organizational assets and systems” where this information could be incorporated.

There is also a cybersecurity component of authentication. Accordingly, relevant information should be included in Section 3.2 for “Establishing or Improving a Cybersecurity Program”, especially in connection with establishing a “Target Profile.” (Our other comments in this response recommend that “Target Profile” needs to be further defined.)

In addition, “PR.AC-1: Identities and credentials are managed for authorized devices and users” should be updated for the “Protect” function in the “Access Control” category of Appendix A: Framework Core.

Automated Indicator Sharing

Section 3 of the Framework (“Use of the Framework”) could benefit from addressing in more detail what “automated indicator sharing” is and the kind of information that is shared across (such as potential network-level and system-level indicators of compromise). The information provided could offer a roadmap for information sharing, both intra-sector and cross-sector, encouraging the goal of holistic, community-based information sharing.

The Roadmap should include components such as the following: (1) interoperable, technical solutions that may be used to conduct the automated indicator sharing, (2) technical solutions to consume the information shared across, and (3) integration of the information with other

cybersecurity systems and platforms, such as intrusion detection systems, intrusion prevention systems, firewalls, and Security Information and Event Management (“SIEM”) systems.

The challenges that small and medium-sized organizations may encounter as a result of funding, resources, and manpower should also be taken into account when developing the NIST Roadmap. Ideally, barriers to information sharing should be mitigated, if not completely eliminated, to enable true holistic, community-based information sharing intra-sector and cross-sector.

On a related note, the Framework could address how “potential indicators of compromise” may be discovered, such as by a person or by a machine. Given the current state of the art, there may be instances wherein a human analyst may be able to discover a potential indicator of compromise that a machine (using an algorithm and/or machine learning) may not be able to discover.

In terms of the content of the current Framework, Section 3.5 (“Methodology to Protect Privacy and Civil Liberties”) could be supplemented by adding automated indicator sharing to the heading “Anomalous activity detection and system and assets monitoring.” Peer-to-peer (i.e., word of mouth) indicator sharing should also be addressed here as well. The [2015 HIMSS Cybersecurity Survey results](#) revealed that most used cyber threat intelligence source was from peers (word of mouth), according to survey respondents. (Peer-to-peer information sharing, in addition to automated indicator sharing, should also be added to Section 3.2 (“Establishing or Improving a Cybersecurity Program”).)

In addition, the “Anomalies and Events (DE.AE)” category for the Detect function and the “Communications (RS.CO)” category for the Respond function of Appendix A could be updated to include automated indicator sharing and peer-to-peer (word of mouth) indicator sharing. With regard to peer-to-peer (word of mouth) indicator sharing, references could be made to the [National Incident Management System](#) (“NIMS”) as well as the [National Response Framework](#) (“NRF”) and the [National Cyber Incident Response Plan](#).

Cybersecurity Workforce

The Framework and, especially Section 3 (“Use of the Framework”) could benefit from an explanation about the people and process components of cybersecurity. People, and the processes they implement, are necessary to perform the entire core functions of the Framework (i.e., identify, protect, detect, respond, and recover). In addition, people and processes are necessary to ensure privacy and civil liberties and so these components should also be addressed in Section 3.5.

Data Analytics

Potential indicators of compromise may be derived from data analytics solutions. Whether the potential indicators of compromise are based upon actual incidents or predictive analysis, the know-how associated with data analytics to produce such threat intelligence should be widely shared so as to help foster best-of-breed automatic indicator sharing systems and platforms.

Technical Privacy Standards

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) Privacy Rule establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The HIPAA Privacy Rule also applies to business associates. Further, the HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

To the extent that Section 3 (“Use of the Framework”) is updated with context specific to the healthcare sector, the HIPAA Privacy Rule could also be incorporated in the discussion regarding use of the Framework. In addition, the HIPAA Security Rule could be incorporated, as appropriate, into the discussion regarding the use of the Framework.

What, if anything, is inhibiting the sharing of best practices?

Before best practices can be shared, there needs to be a common understanding in the sector as to where there will be best practices developed. Section 405 of the Cybersecurity Act of 2015 calls for “a common set of voluntary, consensus-based, and private sector-led guidelines, best practices, methodologies, procedures, and processes.” The foundation (i.e., best practices, guidelines, methodologies, procedures, and processes that are private sector-led) needs to be established first by the healthcare sector by way of a collaborative process that includes a wide array of healthcare sector stakeholders.

What steps could the U.S. government take to increase sharing of best practices?

According to Section 405 of the Cybersecurity Act of 2015, the healthcare industry cybersecurity taskforce will, among other duties, provide the Secretary of the Department of Health and Human Services (HHS) with information to disseminate to healthcare industry stakeholders of all sizes for purposes of improving preparedness and response to cyber threats in healthcare. The healthcare sector could greatly benefit from this information—however, the U.S. government (i.e., NIST and other relevant government agencies) could assist in this effort through wide dissemination of such information across the healthcare sector (including, without limitation, small physician practices, long-term care facilities, and other healthcare organization constituents, large and small).

Also, according to Section 405 of the Cybersecurity Act of 2015, HHS shall establish a collaborative process with the Department of Homeland Security (DHS), healthcare industry stakeholders, and NIST to develop a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes. Healthcare stakeholders should include those well-versed in healthcare cybersecurity. In addition, the healthcare stakeholders with whom the U.S. government collaborates with should include a wide range of healthcare organizations (including, without limitation, small physician practices, long-term care facilities, and other healthcare organization constituents, large and small). Including a critical mass of healthcare stakeholders (as well as a broad range of them) is quintessential, as they will ultimately be the “consumers” of such information.

Finally, the U.S. government could increase sharing of best practices by facilitating cross-sector information sharing as well. The healthcare sector has numerous dependencies upon other critical infrastructure sectors and would greatly benefit from such cross-sector information sharing.

What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?

The program should be accessible to everyone, wherein costs, technical constraints, and logistics are not barriers. Ideally, this program would be available to every stakeholder at no cost.

What should be the private sector's involvement in the future governance of the Framework?

The private sector should be involved in future governance of the Framework to ensure a common set of voluntary, consensus-based, and private sector-led guidelines, best practices, methodologies, procedures, and processes. The Framework should be expanded to address the multiple dependencies of other sectors for each relevant critical infrastructure sector. This is why representatives from each critical infrastructure sector from the private sector need to be involved in governance of the Framework to ensure that its shape and direction are both appropriate and relevant.

Should NIST consider transitioning some or even all of the Framework's coordination to another organization?

HIMSS is neutral on whether some or all of the Framework's coordination should be transitioned to another organization.

If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?

While HIMSS is neutral as to the type of organization that could serve as a transition partner (if the Framework were to be transitioned), the organization should ideally be free of vendor bias and should not benefit from an economic windfall due to products and/or services (including consulting services) relevant to the Framework. Ideally, the organization should also perform its Framework-related functions (including development and update of the Framework) at no cost to participating organizations.

What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?

While there are many factors which could be used to evaluate such capacity, ideally the partner should have an awareness of the unique challenges of the healthcare sector to reduce cyber risk, in addition to an in-depth understanding. Moreover, the transition partner ensure that cost is not a barrier to participation—ideally, the partner should not assess any cost for organizations, including healthcare organizations, to assist with development of or to use the Framework.

HIMSS is committed to being a resource to NIST in its mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life as it relates to the healthcare sector.

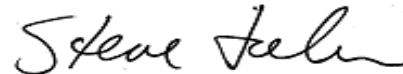
We look forward to the opportunity to further discuss these issues with you in more depth. Please feel free to contact [Jeff Coughlin](#), Senior Director of Federal & State Affairs, at 703.562.8824, or [Eli Fleet](#), Director of Federal Affairs, at 703.562.8834, with questions or for more information.

Thank you for your consideration.

Sincerely,



Alexander RN, MSN, MBA, FAAN, FHIMSS
Vice President, Clinical Transformation
Divurgent
Chair, HIMSS North America Board of Directors



H. Stephen Lieber, CAE
President & CEO
HIMSS